UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/812,622	03/30/2004	Kazumasa Omote	1924.70199	3471

7590 01/11/2008

Patrick G. Burns, Esq.
GREER, BURNS & CRAIN, LTD.
Suite 2500
300 South Wacker Dr.
Chicago, IL 60606

EXAMINER	
JOHNSON, CARLTON	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
01/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

## *Office Action Summary*	**Application No.** 10/812,622	**Applicant(s)** OMOTE ET AL.	
	Examiner Carlton V. Johnson	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _15 October 2007_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-40_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-40_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _8-10-2007 / 10-15-2007_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is responding to application papers filed on **3-20-2004**.

2. Claims **1 - 40** are pending. Claims **1, 5, 7, 9, 12 - 16, 20** have been amended. Claims **21 - 40** are new. Claims **1, 12, 13, 14, 33, 39, 40** are independent.

Response to Arguments

3. Applicant's arguments filed 10/15/2007 have been fully considered but they are moot due to new grounds of rejection.

Responses:

3.1 Applicant argues that the referenced prior art does not disclose, *"extracting referenced information and blocking communications packets". (see Remarks Pages 18, 19)*

The Spiegel prior art discloses retrieving reference information for a communications packet. (see Spiegel col. 4, lines 17-20; col. 4, lines 27-31; col. 4, lines 45-48: calculation address accesses in worm determination) The Spiegel and Willebeek-LeMair prior art combination discloses the specific extraction of reference information from a communications packet. (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (IP address, port number)) And, the Spiegel and Willebeek-LeMair prior art combination discloses blocking a communication packet(s) from entrance to a protected (internal) network segment from an external (outside) network segment. (see Willebeek-LeMair paragraph [0017], lines 12-15; paragraph [0031], lines 5-14; paragraph [0035], lines 7-14: block communications packets between network segments (inside network segment and outside network segment))

3.2 Applicant argues that the referenced prior art does not disclose, *"judging unit, extracting unit". (see Remarks Page 18)*

The Spiegel prior art discloses a software, computer program implementation of the prior art invention. A software implementation implies program module to operate as functional units performing specific functions such as extracting information utilizing an extraction unit and judging criteria utilizing a judging unit. (see Spiegel col. 6, lines 15-24:)

3.3 The examiner has considered the applicant's remarks concerning a communication-information acquisition section acquires information related to an address of a communication packet based on setting information stored in the setting-data. Worm detection section makes a judgment of whether a communication is executed by a worm, based on information acquired by the communication-information acquisition section and related to the judgement criteria that is stored in the setting-data. Applicant's arguments have thus been fully analyzed and considered but they are not persuasive.

After an additional analysis of the applicant's invention, remarks, and a search of the available prior art, it was determined that the current set of prior art consisting of Spiegel et al. (7,159,149), Willebeek-LeMair et al. (US PGPUB No. 20030204632) and Bunker, V et al. et al. (US PGPUB No. 20030056116) discloses the applicant's invention including disclosures in Remarks dated October 15, 2007.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims **1 - 11, 21, 25, 29** have been rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claimed computer program product may or may not be executable since it fails to include a computer readable medium as part of the product. The product could be interpreted as descriptive material.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims **1 - 24, 29 - 34, 36 - 40** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Spiegel et al.** (US Patent No. **7,159,149**) in view of **Willebeek-LeMair et al.** (US PGPUB No. **20030204632**).

Regarding Claims 1, 13, 14, Spiegel discloses a computer program, device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, causes a computer to perform:

a) acquiring information related to a traffic and a communication address of a communication packet based on setting information; (see Spiegel col. 2, lines 51-53; col. 2, lines 62-65; col. 6, lines 15-22: software, implementation means; col. 1, lines 50-60; col. 3, lines 27-30: monitor network traffic based on source and destination addresses and information not matching criteria for normal traffic setting) and

b) judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria; (see Spiegel col. 1, lines 60-67; col. 3, line 63 - col. 4, line 9: determine communications due to worm, based on threshold or predetermined criteria)

Spiegel does not specifically disclose extracting reference information for identifying a communication packet, and blocking the communication packet as part of worm determination.

However, Willebeek-LeMair discloses:

c) extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm; (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (IP address, port number)) and

d) blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting. (see Willebeck-LeMair paragraph [0017], lines 12-15; paragraph [0031], lines 5-14; paragraph [0035], lines 7-14: block communications packets between network segments (inside network segment and outside network segment))

It would have been obvious to one of ordinary skill in the art to modify Spiegel as taught by Willebeek-LeMair to enable the capability to block network access after a determination of a worm has been judged. One of ordinary skill in the art would have been motivated to employ the teachings of Willebeek-LeMair in order to enable the capability to threat detection and threat response operational in an optimized manner that mitigates false detection. (see Willebeek-LeMair paragraph [0013], lines 5-11: *" ... Self-deployed security defense is achieved by having the included defense functionalities work together to automate threat detection and threat response operations. Self-hardening security defense is achieved by having the included functionalities implement threat detection and threat response operations in an optimized manner that mitigates instances of false detection. ... "*)

Regarding Claims 2, 15, Spiegel discloses the computer program, device according to claims 1, 14, causes the computer to further perform changing the setting information upon it being judged at the judging that the communication is executed by the worm, wherein the acquiring includes acquiring the information based on the setting information after change. (see Spiegel col. 5, lines 15-21: dynamic (i.e. adjustable, changeable) parameters for worm determination; col. 6, lines 15-22: software, implementation means)

Regarding Claims 3, 16, Spiegel discloses the computer program, device according to claims 1, 14, causes the computer to further perform changing the judgment criteria upon it being judged at the judging that the communication is executed by the worm, wherein the judging includes judging whether the communication is executed by the worm based on the information acquired and the setting information after change. (see Spiegel col. 5, lines 8-10; col. 5, lines 15-21: worm determination based on information and adjusted (i.e. changed) information; col. 6, lines 15-22: software, implementation means)

Regarding Claims 4, 17, Spiegel discloses the computer program, device according to claims 1, 14, wherein the judging includes judging that a communication from a computer that is in the predetermined network segment is executed by the worm when there is an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside. (see Spiegel col. 3, lines 20-27: network communication packets throughput increased, worm determination; col. 6, lines 15-22: software, implementation means)

Regarding Claims 5, 18, Spiegel discloses the computer program, device according to claim 4, 17, wherein the judging includes judging that a communication from a plurality of computers in the predetermined segment is executed by the worm when

a) a communication from a computer in the predetermined network segment is judged previously to be executed by the worm, (see Spiegel col. 5, lines 8-10: history of worm detection; col. 5, lines 47-50: particular source/destination addresses (i.e. for a computer) monitored; col. 6, lines 15-22: software, implementation means) and

b) the number of destination addresses of the communication packet that is transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of a communication packet acquired when the communication is judged to be executed by the worm, and is transmitted from the predetermined network segment to the outside. (see Spiegel col. 3, lines 20-27: worm determination based on number of packets transferred to addresses (i.e. inside or outside local network))

Regarding Claims 6, 19, Spiegel discloses the computer program, device according claims 1, 14, wherein the judging includes judging that a communication from a computer that is outside the predetermined network segment is executed by the worm when

a) there is an increase in number of responding communication packets corresponding to communication packets that are transmitted from outside to the predetermined network segment, (see Spiegel col. 4, lines 17-22: communications increase (i.e. inside or outside local network), worm determination; col. 6, lines 15-22: software, implementation means) and

b) there is an increase in number of sender addresses of the communication packets. (see Spiegel col. 3, lines 20-27: communications (i.e. address, and process port number) increases, worm determination)

Regarding Claims 7, 20, Spiegel discloses the computer program, device according to claims 1, 14, wherein the judging includes outputting any one of information about a computer that performed the communication and a communication status upon it being judged that the communication is executed by the worm. (see Spiegel col. 3, lines 58-63; col. 4, lines 11-16: source address (i.e. for a computer) a factor in worm determination; col. 6, lines 15-22: software, implementation means)

Regarding Claim 8, Spiegel discloses the computer program according to claim 1, wherein the judging includes predicting a type of the worm by comparing features of a communication judged to be executed by a worm with features of a communication executed by a worm that is recorded in advance. (see Spiegel col. 3, lines 58-67: worm determination; col. 5, lines 8-15: history or recorded information utilized in worm determination; col. 6, lines 15-22: software, implementation means)

Regarding Claim 9, Spiegel discloses the computer program according to claim 1, causes the computer to perform cutting off the communication executed by the worm upon it being judged that the communication is executed by the worm. (see Spiegel col. 2, lines 13-18: terminate network access (i.e. cut off communications), worm determination; col. 6, lines 15-22: software, implementation means)

Regarding Claim 10, Spiegel discloses the computer program according to claim 9, wherein the cutting off includes cutting off the communication executed by the worm by stopping a process that is started by the worm. (see Spiegel col. 2, lines 13-18: terminate affected process (i.e. stopping a process), worm determination; col. 6, lines 15-22: software, implementation means)

Regarding Claim 11, Spiegel discloses the computer program according to claim 9, wherein the cutting off includes cutting off the communication executed by the worm by making a fire wall function effective in a computer that is judged to have a worm. (see Spiegel col. 6, lines 48-55: firewall functioning; col. 6, lines 15-22: software, implementation means)

Regarding Claim 12, Spiegel discloses the computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

a) acquiring information related to a traffic and a communication address of a communication packet based on setting information; (see Spiegel col. 2, lines 51-53; col. 2, lines 62-65; col. 6, lines 15-22: software, implementation means; col. 1, lines 50-60; col. 3, lines 27-30: monitor network traffic based on source and destination addresses) and

b) judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria; (see Spiegel col. 1, lines 60-67; col. 3, line 63 - col. 4, line 9: determine communications based on worm, threshold criteria)

Spiegel does not specifically disclose extracting reference information for identifying a communication packet, and blocking the communication packet as part of worm determination.

However, Willebeek-LeMair discloses:

c) extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm; (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (IP address, port number)) and

d) blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting. (see Willebeck-LeMair paragraph [0017], lines 12-15; paragraph [0031], lines 5-14; paragraph

[0035], lines 7-14: block communications packets between network segments (inside network segment and outside network segment))

It would have been obvious to one of ordinary skill in the art to modify Spiegel as taught by Willebeek-LeMair to enable the capability to block network access after a determination of a worm has been judged. One of ordinary skill in the art would have been motivated to employ the teachings of Willebeek-LeMair in order to enable the capability to threat detection and threat response operational in an optimized manner that mitigates false detection. (see Willebeek-LeMair paragraph [0013], lines 5-11)

Regarding Claims 21, 22, 23, 24, 34, Spiegel discloses the computer program, computer-readable medium, method, device according to claims 1, 12, 13, 14, 33. (see Spiegel col. 1, lines 48-62: monitoring for worm determination; col. 4, lines 45-48: traffic analysis, calculation utilizing network addressing (IP address, port number)) Spiegel does not specifically disclose extracting a port number. However, Willebeek-LeMair discloses wherein the extracting includes extracting as the reference information, a most frequently appearing port number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging. (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (IP address, port number))

It would have been obvious to one of ordinary skill in the art to modify Spiegel as taught by Willebeek-LeMair to enable the capability for extracting a port number in determination of a worm. One of ordinary skill in the art would have been motivated to employ the teachings of Willebeek-LeMair in order to enable the capability to threat detection and threat response operational in an optimized manner that mitigates false detection. (see Willebeek-LeMair paragraph [0013], lines 5-11)

Regarding Claims 29, 30, 31, 32, 36, Spiegel discloses the computer program, computer-readable medium, method, device according to claims 1, 12, 13, 14, 33. (see Spiegel col. 1, lines 48-62: monitoring for worm determination; col. 4, lines 45-48: traffic analysis, calculation utilizing network addressing (IP address, port number)) Spiegel does not specifically disclose extracting an address in worm determination. However, Willebeek-LeMair discloses wherein the extracting further includes detecting address information of a worm-infected computer from a header of the communication packet transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting the address information as the reference information. (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (addressing: IP addresses, port number))

It would have been obvious to one of ordinary skill in the art to modify Spiegel as taught by Willebeek-LeMair to enable the capability for extracting an address in determination of a worm. One of ordinary skill in the art would have been motivated to employ the teachings of Willebeek-LeMair in order to enable the capability to threat detection and threat response operational in an optimized manner that mitigates false detection. (see Willebeek-LeMair paragraph [0013], lines 5-11)

Regarding Claim 33, Spiegel discloses a device for cutting off a communication executed by a worm by monitoring the communication between a predetermined network segment and outside of the predetermined network segment, comprising:

a) a worm judging unit that judges whether a communication is executed by the worm; (see Spiegel col. 1, lines 60-67; col. 3, line 63 - col. 4, line 9: determine communications due to worm, based on threshold or predetermined criteria)

Spiegel does not specifically disclose extracting reference information for identifying a communication packet, and blocking the communication packet as part of worm determination.

However, Willebeek-LeMair discloses:

b) a reference information extracting unit that extracts reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged by the worm judging unit that the communication is executed by the worm; (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (IP address, port number)) and

c) a blocking unit that blocks the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted by the reference information extracting unit. (see Willebeek-LeMair paragraph [0017], lines 12-15; paragraph [0031], lines 5-14; paragraph [0035], lines 7-14: block communications packets between network segments (inside network segment and outside network segment))

It would have been obvious to one of ordinary skill in the art to modify Spiegel as taught by Willebeek-LeMair to enable the capability to block network access after a determination of a worm has been judged. One of ordinary skill in the art would have been motivated to employ the teachings of Willebeek-LeMair in order to enable the capability to threat detection and threat response operational in an optimized manner that mitigates false detection. (see Willebeek-LeMair paragraph [0013], lines 5-11)

Regarding Claim 37, Spiegel discloses the device according to claim 33, wherein the worm judging unit judges whether the communication is executed by the worm based on traffic of the communication packets transmitted in the communication. (see Spiegel col. 1, lines 48-62: communications determined to executed by a worm)

Regarding Claim 38, Spiegel discloses the device according to claim 33, wherein the worm judging unit judges whether the communication is executed by the worm based on the information related to a communication address of a communication packet transmitted in the communication. (see Spiegel col. 1, lines 48-62: worm determination; col. 4, lines 17-20; col. 4, lines 27-31; col. 4, lines 45-48: address utilized in worm determination)

Regarding Claim 39, Spiegel discloses a computer-readable recording medium for storing a computer program for cutting off a communication executed by a worm by monitoring the communication between a predetermined network segment and outside of the predetermined network segment, the computer program causing a computer to perform:

a) judging whether a communication is executed by the worm; (see Spiegel col. 1, lines 60-67; col. 3, line 63 - col. 4, line 9: determine communications due to worm, based on threshold or predetermined criteria)

Spiegel does not specifically disclose extracting reference information for identifying a communication packet, and blocking the communication packet as part of worm determination.

However, Willebeek-LeMair discloses:

b) extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm; (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (IP address, port number)) and

c) blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting. (see Willebeck-LeMair paragraph [0017], lines 12-15; paragraph [0031], lines 5-14; paragraph [0035], lines 7-14: block communications packets between network segments (inside network segment and outside network segment))

It would have been obvious to one of ordinary skill in the art to modify Spiegel as taught by Willebeek-LeMair to enable the capability to block network access after a determination of a worm has been judged. One of ordinary skill in the art would have been motivated to employ the teachings of Willebeek-LeMair in order to enable the capability to threat detection and threat response operational in an optimized manner that mitigates false detection. (see Willebeek-LeMair paragraph [0013], lines 5-11)

Regarding Claim 40, Spiegel discloses a method for cutting off a communication executed by a worm by monitoring the communication between a predetermined network segment and outside of the predetermined network segment, comprising:

a) judging whether a communication is executed by the worm; (see Spiegel col. 1, lines 60-67; col. 3, line 63 - col. 4, line 9: determine communications due to worm, based on threshold or predetermined criteria)

b) extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm; (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (IP address, port number)) and

c) blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting. (see Willebeck-LeMair paragraph [0017], lines 12-15; paragraph [0031], lines 5-14; paragraph [0035], lines 7-14: block communications packets between network segments (inside network segment and outside network segment))

It would have been obvious to one of ordinary skill in the art to modify Spiegel as taught by Willebeek-LeMair to enable the capability to block network access after a determination of a worm has been judged. One of ordinary skill in the art would have been motivated to employ the teachings of Willebeek-LeMair in order to enable the capability to threat detection and threat response operational in an optimized manner that mitigates false detection. (see Willebeek-LeMair paragraph [0013], lines 5-11)

8. Claims **25, 26, 27, 28, 35** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Spiegel-Willebeek-LeMair** and further in view of **Bunker et al.** (US PGPUB No. **20030056116**).

Regarding Claims 25, 26, 27, 28, 35, Spiegel discloses the computer program, computer-readable medium, method, device according to claims 1, 12, 13, 14, 33. (see Spiegel col. 1, lines 48-62: monitoring for worm determination; col. 4, lines 45-48: traffic analysis, calculation utilizing network addressing (IP address, port number)) Spiegel does not specifically disclose calculations utilizing reference information such as port numbers in the analysis of work determination. However, Bunker discloses wherein the extracting further includes summing up, for each type of the communication, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a type of the communication wherein the number of the communication packets is over a threshold value. (see Bunker paragraph [0189], lines 1-11; paragraph [0215], lines 1-5; paragraph [0220], lines 8-12: calculation (summation) of access information in worm determination)

It would have been obvious to one of ordinary skill in the art to modify Spiegel as taught by Bunker to enable the capability to calculate a summation of reference information utilized for worm determination. One of ordinary skill in the art would have been motivated to employ the teachings of Bunker in order to enable the capability to emulate hacker methodology in a safe way and enable study of dnetwork security openings without affecting customer operations. (see Bunker paragraph [0012], lines 1-8: " *... To answer the security needs of the market, a preferred embodiment was developed. A preferred embodiment provides real-time network security vulnerability assessment tests, possibly complete with recommended security solutions. External vulnerability assessment tests can emulate hacker methodology in a safe way and enable study of a network for security openings, thereby gaining a true view of risk level without affecting customer operations. ...* ")

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/7/08

C.J.
CVJ
December 26, 2007